沖縄ICTフォーラム2015 in 石垣島

東京2020大会に向けたサイバーセキュリティの準備について

平成27年7月9日

公益財団法人　東京オリンピック・パラリンピック競技大会組織委員会
テクノロジーサービス局　局長　　舘　剛司

自己紹介

舘　剛司（たち　たけし）
東京オリンピック・パラリンピック競技大会組織委員会　テクノロジーサービス局　局長

略歴：

1989年、大阪大学　大学院工学研究科　電気工学・修士課程修了。同年、日本電信電話株式会社（NTT）入社。

1995年まで、映像伝送サービスにおける品質評価法の研究、映像伝送システムの開発などに従事。

1997年、米国カリフォルニア大学バークレー校　経営工学・修士課程修了。

1998年より、次世代IPネットワークの開発、サイバーセキュリティ分野の研究開発戦略の策定などに従事。

2007年より、オープンソースソフトウェアに関する外部アライアンス戦略策定、知的財産に関する戦略策定などに従事。

2013年より、米国のR&D子会社（NTT Innovation Institute, Inc.）設立とサイバーセキュリティ分野のR&D計画管理に従事。

2014年より組織委員会へ出向し、2020年大会の運営や準備活動に必要なネットワーク・情報システムなど技術全般に関する計画策定、開発、運用、サポートなどを統括。

本日のアジェンダ

1. 2020年大会に際して、どのようなリスクを想定すべきか？
2. “2020年大会を守る”とは？
3. 組織委員会のアプローチ
4. サイバーセキュリティにおける大会のレガシーとは？（考察）

1. 2020年大会に際して、どのようなリスクを想定すべきか？

大会ネットワークの規模感（ロンドン大会の場合注）)

✓ スタッフの規模感
- 組織委員会スタッフ　8,000名／その他大会運営に関わったスタッフ　70,000名

✓ ネットワークの規模感
- 英国内100以上のロケーションにまたがる大会用ネットワークを構築
- 大会関係者に提供された通信サービス：Eメール、インターネット、ビデオ/Web会議、IP電話、携帯電話、業務用無線、など

✓ 情報システムの規模感
- 大会関係者に発行されたアクレディテーションカード　25,000名分（組織委員会、IOC、IPC、競技団体、アスリート、コーチ、放送局、メディア、スポンサー、ボランティアなど）
- オリンピック26競技302種目、パラリンピック20競技503種目の競技結果をリアルタイムに放送局・メディアに提供
- 競技スケジュール、天候、輸送などに関わる情報を、14,700人のアスリートに提供

注）統計によって数字は若干異なります。

IOCが要求するサイバーセキュリティ

- ✓ 守るべきシステムを5つのカテゴリーで整理
  - [1] 組織委員会が自ら構築するシステム（組織委員会ネットワークなど）
  - [2] 組織委員会が利用する外部システム（クラウド環境など）
  - [3] 大会運営に直接関わる組織委員会以外のシステム（電力、インターネットなど）
  - [4] 間接的に関わる組織委員会以外のシステム（交通機関など）
  - [5] 関連はあるが非重要なシステム（スポンサーの社内ネットワークなど）

- ✓ 上記すべてにわたって政府関係機関と連携し、コーディネーションが必要

IOCが推奨する5つの対策

- ✓ 組織委員会として基礎を固める（戦略・方針、アーキテクチャ、組織文化など）
- ✓ 過去のベストプラクティスの採用（政府のセキュリティ基準、繰り返しのペネトレ試験など）
- ✓ 基本に忠実に（リスク評価、可視化、パッチあてオペレーションなど）
- ✓ 政府機関、インテリジェンス機関との連携
- ✓ マネージドサービスの活用

過去大会でも想定されていたリスク（例）

分類	項目	備考
金銭目的のサイバー犯罪	偽チケット販売サイト	国内だけでなく海外でも想定される
	フィッシング、偽サイト、偽アクセスポイントなどによる個人情報の搾取	
	ランサムウェアによる脅迫	
ハクティビストの攻撃	大会サイトへの攻撃（DoS攻撃、改ざん）	大会に関するメディア報道、国の記念日、ネガティブ・キャンペーン、関連イベント開催などがきっかけ
	スポンサーや開催都市など関連サイトへの攻撃	周辺サイトがとばっちりを受けやすい
	競技対戦国の関連サイトへの攻撃	近年のスポーツイベントにつきもの
サイバーテロ	大会システムへの侵入によるシステム破壊、データ破壊	狙われるかどうかは、大会開催時の国内外の情勢に依存
	大会システムの乗っ取り	
	重要インフラへのサイバー攻撃	
サイバー戦争	要人を狙ったサイバースパイ	海外要人も多数来訪するため

東京2020大会で想定される環境の変化

社会全体のますますのIT化

- モバイル端末の進化・普及により、ロンドン大会より桁違いに大きい通信トラヒック
- ネットワークにつながるものが急激に増加することに伴うリスクの広域化・複雑化

国際情勢の変化

- サイバーテロやサイバー戦争に巻き込まれるリスク

大会システム・放送システムの進化

- インターネットやクラウドへの依存度の増加
- 放送システムのIP技術の採用

関係機関どうしの連携の重要性

- リスクの広域化・複雑化に伴い、一組織・機関に閉じてできる対策の限界

東京2020大会で新たに懸念されるリスク（想定例）

競技システム	携帯電話OSの脆弱性を悪用した大会用アプリケーションの改ざんによる運営の混乱	競技関係者が利用するウエアラブルデバイスの脆弱性を利用した乗っ取りによる競技結果の改ざん
競技場インフラ	IP化が進む放送システムを狙った攻撃による放送中断	セキュリティカメラシステムのハッキングによるテロ
周辺インフラ	競技場のビル管理システムへのハッキングによる運営の混乱	公共システムへのハッキングを利用したパニック誘発（炎天下での空調システム、台風・ゲリラ豪雨での避難誘導、渋滞時の交通システムなど）

2. “2020年大会を守る”とは？

東京2020大会に向けて、何を準備する必要があるのか？

【ポイント1】 50年に一度の大きなイベントに備え、潜在的な課題に早く気づく。

- ✓ これまでは「発生確率が低い」と見なされ、組織の危機対応マニュアルで想定していない“危機”がある。
- ✓ 一方で、**“オリンピックを守る”とはどういうことか**、必ずしもコンセンサスがあるわけではない。

東京2020大会に向けて、何を準備する必要があるのか？

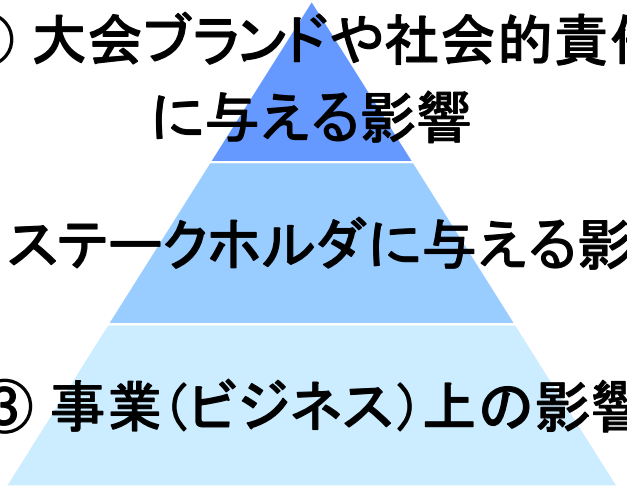
【ポイント2】 サイバーセキュリティは経験則が通用しない。基本に立ち返った検討を。

- ✓ 急激なネットワーク化、新たなICTの台頭などを受け、毎年のように新たなサイバーセキュリティ脅威、攻撃手法が発生している。
- ✓ サイトテロや自然災害などのリスクとは比べ物にならない複雑性・専門性をはらんで来ており、もはや一部の専門家や単一のソリューションに任せればいいものではない。
- ✓ リスク分析や対策検討にあたっては、**方法論から整理する必要**がある。

オリンピックを守るとは？

組織委員会から見たBIA(Business Impact Analysis)（案）

「オリンピックにおける最大のリスクとは、結局はレピュテーションリスクに尽きるだろう。」
（Mr. Oliver Hoare, ロンドン大会における英国内務省所属の大会全体のセキュリティ責任者）



- オリンピック憲章でうたう根本原則に反しない。
- オリンピック・ムーブメントを具現化する。
- パラリンピックについても同様に重視する。

- ステークホルダ（放送局、競技団体など）に迷惑をかけない。
- 円滑に大会を運営する。

- 赤字を出さない／法律を守る／けが人・病人を出さない／サステナビリティに則う／レガシーを残す

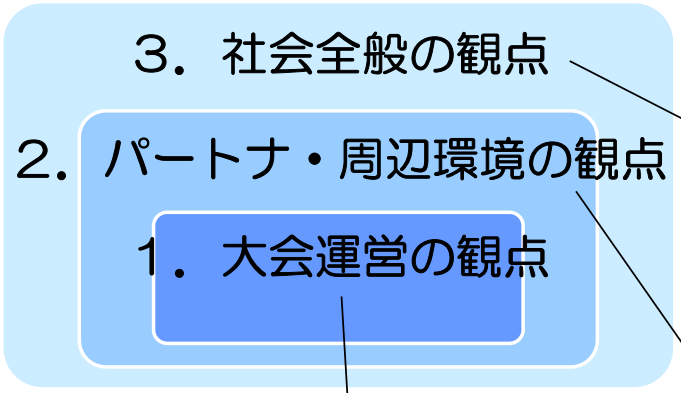
（注）本ページの記載内容は、サイバーセキュリティ対策検討用の仮評価結果であり、実際の評価と異なる可能性があります。

大会システムや大会運営だけ守ればいいのか？

- ✓ 一部の大会オペレーションはインターネットにも依存している。
- ✓ 大会システム、大会用ネットワークが安定して稼働するためには、周辺の社会インフラそのものが安全でなければならない。
- ✓ 大会Webサイトだけ守れても、大会期間中に東京のインターネットバンキングや行政サービスサイトがダウンすれば、東京大会としてのレピュテーションは守れない。
- ✓ 競技スケジュールは順調に進行できても、会場周辺でパニックが起これば大会関係者にも多大な迷惑をかける。
- ✓ 厳重な手荷物検査で会場内のセキュリティは守れても、炎天下で長時間の入場待ちをした大勢の観客は病気になりかねない。

守るべき対象は？

想定リスクの全体像



2020年に狙われやすいのは、むしろ大会システムの周辺環境や日本社会のインフラ、関連企業のサイトである可能性もある。

間接的に大会への影響が懸念されるもの

- *対象リスク事例＝自然災害／パンデミック／社会基盤に対するテロ・サイバーテロ／SNS上での日本・東京に対する評価・評判／RUGBY 2019へのテロ*

組織委員会の管轄範囲内で、大会運営に直接影響するもの

- *対象リスク事例＝観客の動線管理／選手村での食事提供／大会システムへのハッキング／内部情報漏えい／予算不足に伴う運用レベルの低下*

パートナや周辺環境の問題で、大会への影響が大きいもの

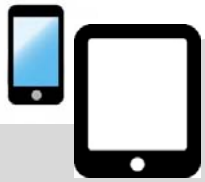
- *対象リスク事例＝災害に伴う避難誘導／サプライチェーン内在リスク／偽チケット販売サイト／重要インフラの障害・停止／会場周辺でのパニック／参加国のボイコット／ドーピング*

大会成功に向けて社会が抱える課題

- ✓ 日本の通信環境（インターネット、公衆WiFiなど）の課題
- ✓ モバイルトラヒックの急増に伴う課題
- ✓ ネットワークにつながるモノ（IoT）が急激に増加していることに伴うルール・体制の課題
- ✓ サイバーセキュリティ人材不足に関する課題
- ✓ 関係機関における情報収集・情報共有に関する課題
- ✓ 関係各国との連携体制に関する課題

日本の社会インフラの安全性が大会の成功をささえる

✓ 2020年は大会と直接関係あるなしに関わらず、東京や日本への注目が集まる機会となる。



急増するモバイルトラヒック
に耐えうるネットワーク

安心・安全なインターネット環境

サイバーセキュリティの人材

大会の成功

関係機関との協力体制

関係各国との連携体制

重要インフラの安全性・安定性

日本の社会インフラ

新しい社会インフラの安全性

JAIPA殿、会員企業殿への期待

- ✓ 日本・東京における安心・安全なインターネット環境の整備
- ✓ 日本・東京における他業界への（民間レベルでの）啓発活動
- ✓ 日本のネット環境・ICT環境のレベルアップに向けたリーダシップ

3. 組織委員会のアプローチ

組織委員会が何らかの形で関与するシステム・ネットワーク

✓ ５つのカテゴリーごとに守るべきシステム・ネットワークを特定

[1] 組織委員会が自ら構築するシステム

- 大会用ネットワーク／競技情報・競技運営システム／業務システム／公式Webサイトなど

[2] 組織委員会が利用する外部システム

- Eメールシステム／スケジューラ・グループウエア／携帯電話／チケット管理システムなど

[3] 大会運営に直接関わる組織委員会以外のシステム

- インターネット／電力／競技場ビル管理システムなど

[4] 間接的に関わる組織委員会以外のシステム

- 公共交通機関／航空管制システム／気象予測システムなど

[5] 関連はあるが非重要なシステム

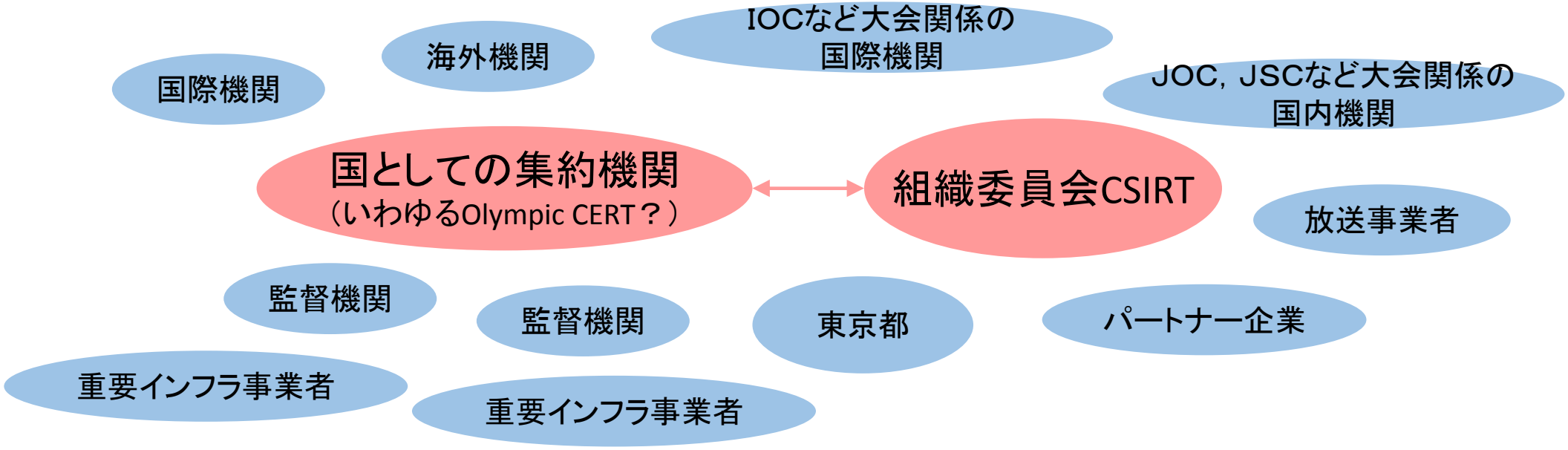
- スポンサー企業の公開Webサイトなど

（注）上記の事例はあくまで説明用の仮定であり、実際の環境を保証するものではありません。

組織委員会がとるべきアプローチ

- ✓ 特定のシステムやネットワークを守るだけでは不十分。組織委員会の事業（ビジネス）である大会オペレーションや大会のレピュテーションを守るという目標設定が必要。
- ✓ 関わるシステム、ネットワークが多いため、対策実施のまえに全体のセキュリティ・アーキテクチャを明確化する必要がある。
- ✓ インターネットをはじめとする社会インフラそのものが安全でなければ、大会も成功しない。関係業界、行政機関、国際機関、近隣諸国などにも協力を仰ぐべき。
- ✓ サイバーテロに備えるためには、政府機関と密に連携したうえでのインテリジェンスも必要。

関係機関との連携におけるポイント



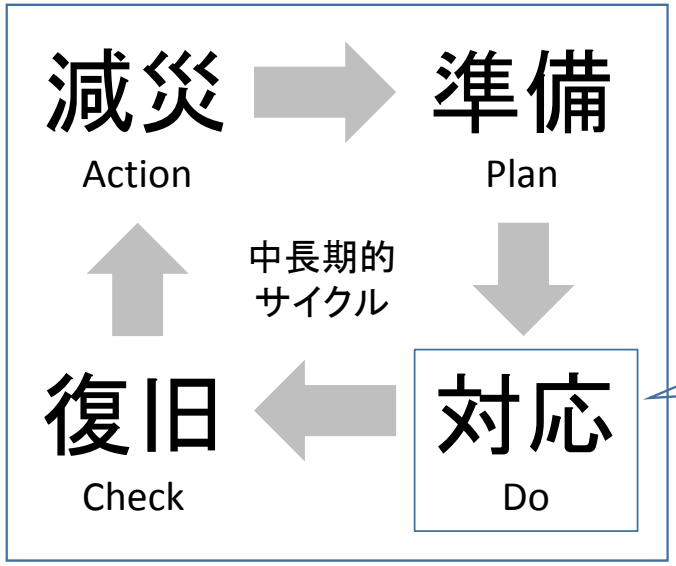
- ✓ “連携”は図に書いて（ルールを決めて）指示するだけでは進みません。
- ✓ **相手の“顔”が見えていること、個人間の“信頼関係”があること、**がいざという時に連携が機能する必要条件です。

事業継続および危機対応のマネジメント・サイクル

ISO22301（事業継続マネジメントシステム）／ISO22320（危機対応に関する要求事項）

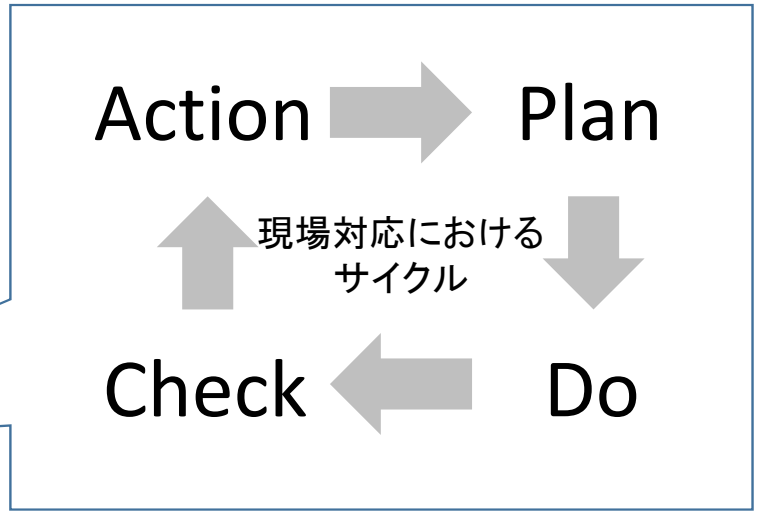
事業継続のマネジメント・サイクル

ISO22301（国際標準）／NIMS（米国政府によるフレームワーク）



危機対応のマネジメント・サイクル

ISO22320（国際標準）／ICS（NIMSで適用が求められている）



NIMS（National Incident Management System）
ICS（Incident Command System）

ISO22320（緊急事態管理―危機対応に関する要求事項）とは？

- ✓ 国家レベルであらゆる災害・危機に対して、効果的に災害・危機対応できる一元的な災害・危機対応システム としてICS（Incident Command System）がある。
  - ➢ 1970年代に米国カリフォルニア州で発生した森林 火災において、指揮統制系統の混乱や、複数の関係機関の間で用語の不統一が 迅速な災害・危機対応のさまたげになったという反省から開発されたもの。
- ✓ これをベースに、テロやハリケーンなどの災害での経験も反映し、標準的な災害・危機対応の仕組みを米国危機管理体制（NIMS: National Incident Management System） が確立。
- ✓ これらの知見をもとに、災 害・危機対応の際に、組織や国を超えて業務を効果的・効 率的に遂行するための最小限の要求事項がISO22320（2011年11月発行、2013年10月にJIS規格化）

災害・危機対応における日米の考え方の違い

日本

- ✓国・公共機関・地方公共団体・事業者・住民それぞれの役割を明確に。
- ✓平時の業務の延長上に災害・危機対応を位置付け。
- ✓**平時の指揮統制の対応能力を超える災害・危機に対しては十分に機能しない可能性も。**

米国

- ✓災害規模に応じて国やさまざまな組織が柔軟に連携する仕組み。
- ✓巨大災害の発生時に、大統領による災害宣言によって連邦政府の機関（アメリカ合衆国連邦緊急事態管理庁）が災害・危機対応業務を直接指揮・統制。
- ✓郡・市においても、対応能力を超えるような災害・危機 発生時には、州が代わって直接物資やサービスを提供。
- ✓企業（NPOを含む）・ボランティアを地域の一部として位置付け。

【出展】“災害・危機対応における日米比較と国際規格ISO22320” 東田光裕、小阪尚子、前田裕二、NTT技術ジャーナル2013.3.
http://www.ntt.co.jp/journal/1303/files/jn201303048.pdf￥

災害・危機対応において露呈しやすい課題

- ✓ １人の管理者に報告が過度に集中する。
- ✓ 対応組織の体制に違いがある。
- ✓ 信頼できる災害情報が得られない。
- ✓ 通信手段が不十分で互換性に欠ける。
- ✓ 関係機関の間で計画を連携させる体制が構築されていない。
- ✓ 権限の境界がはっきりしていない。
- ✓ 関係機関の間で使用している用語に違いがある。
- ✓ 災害・危機対応での目標が不明確で具体性に欠ける。

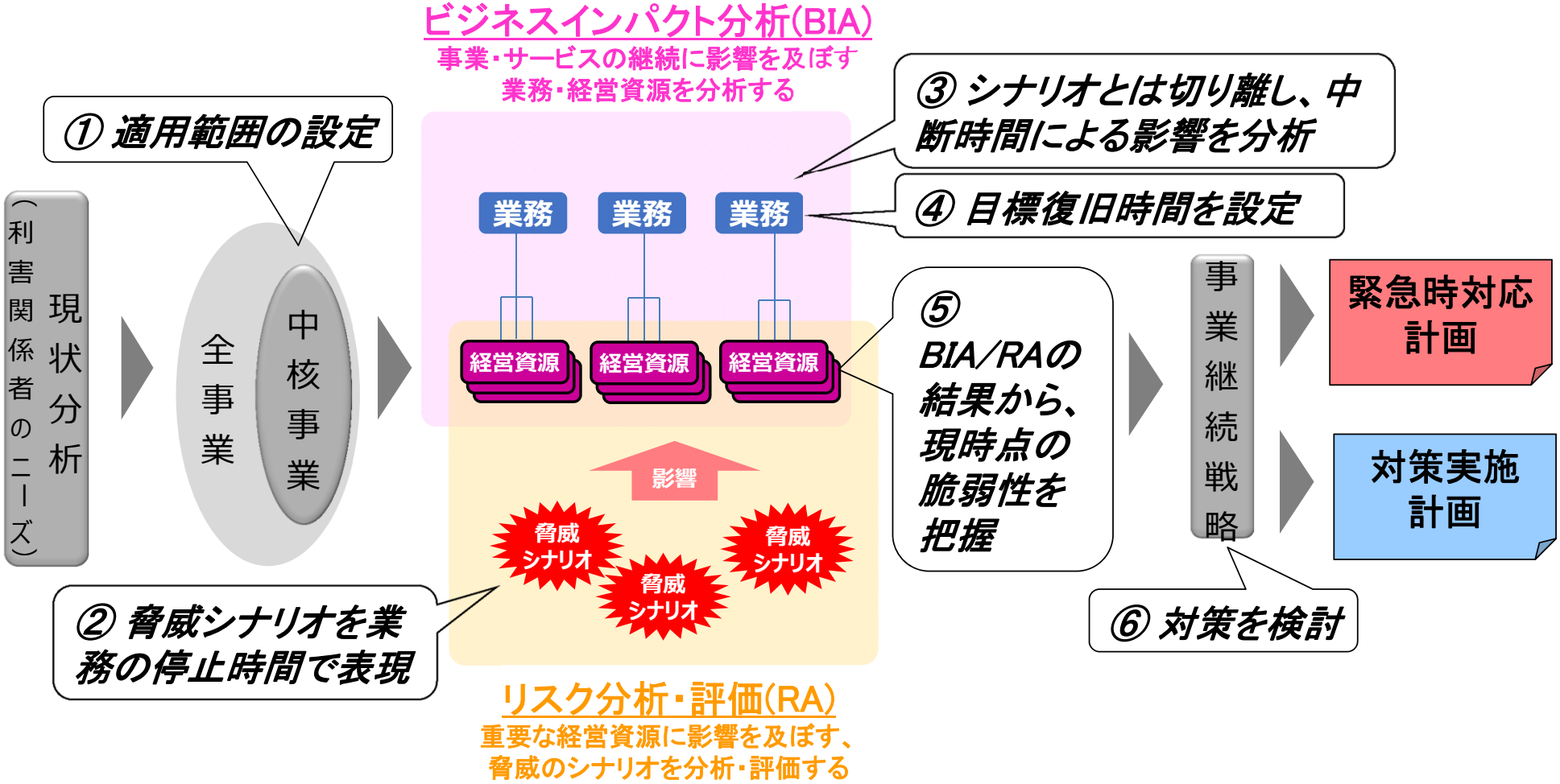
組織に求められる危機対応のための要求条件

① 災害・危機対応にかかわるそれぞれの組織における「指揮・統制（Command and Control）」に関する組織体制および手続きの規定

② 災害・危機対応を進めるために必要となる「活動情報（Operational Information）」を効果的に活用する情報処理のあり方

③ 災害・危機対応にかかわる組織間の「協力と連携（Cooperation and Coordination）」

事業継続性の検討フロー

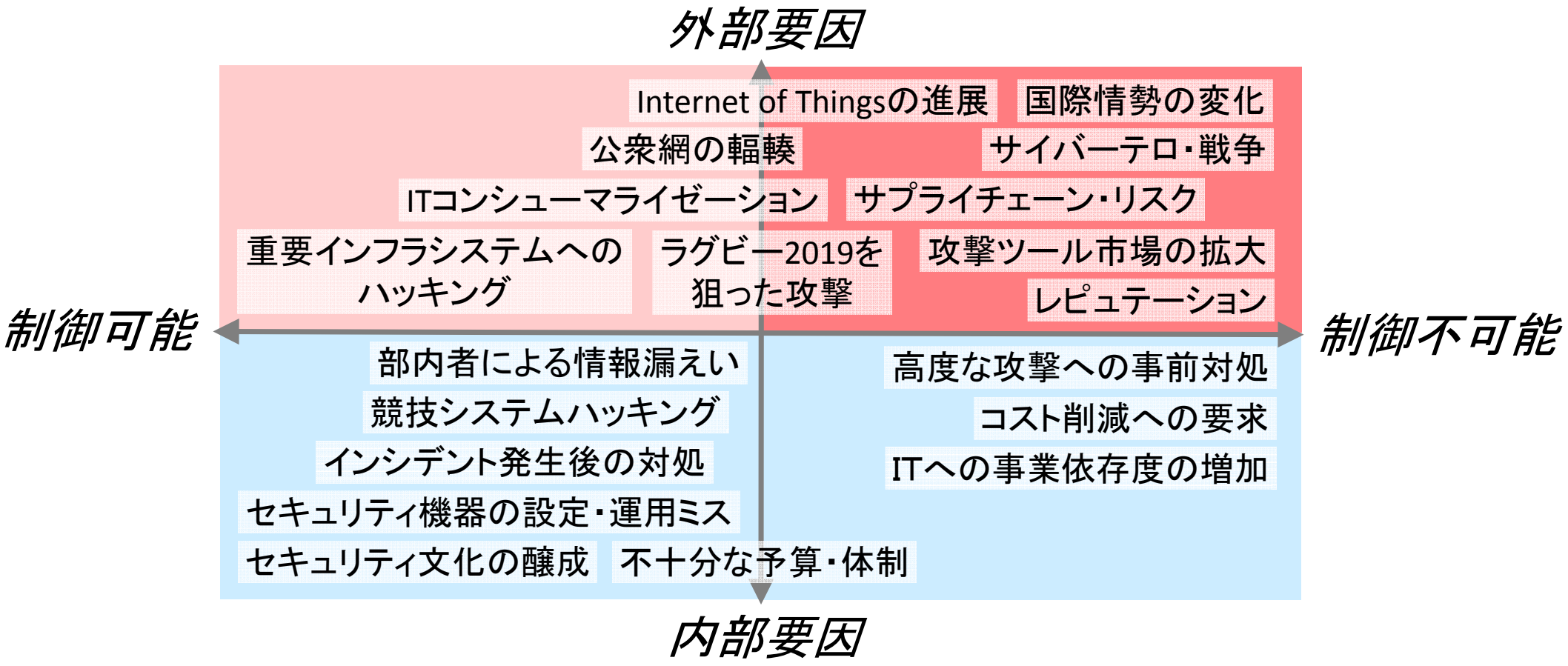


リスク・アーキテクチャの作成

- ✓ 想定される個々のリスクの相関関係・要因の分析などにも踏み込んだ上で、**全体的なリスク・アーキテクチャ（全体像マップ）を作成**する。
  - ➢ 個々の対策の詳細に踏み込む前に（と並行して）、全体像をとらえる営みがまず必要。
  - ➢ 特に“社会全般の観点”では、関係機関（政府、東京都など）との共同検討が必須。

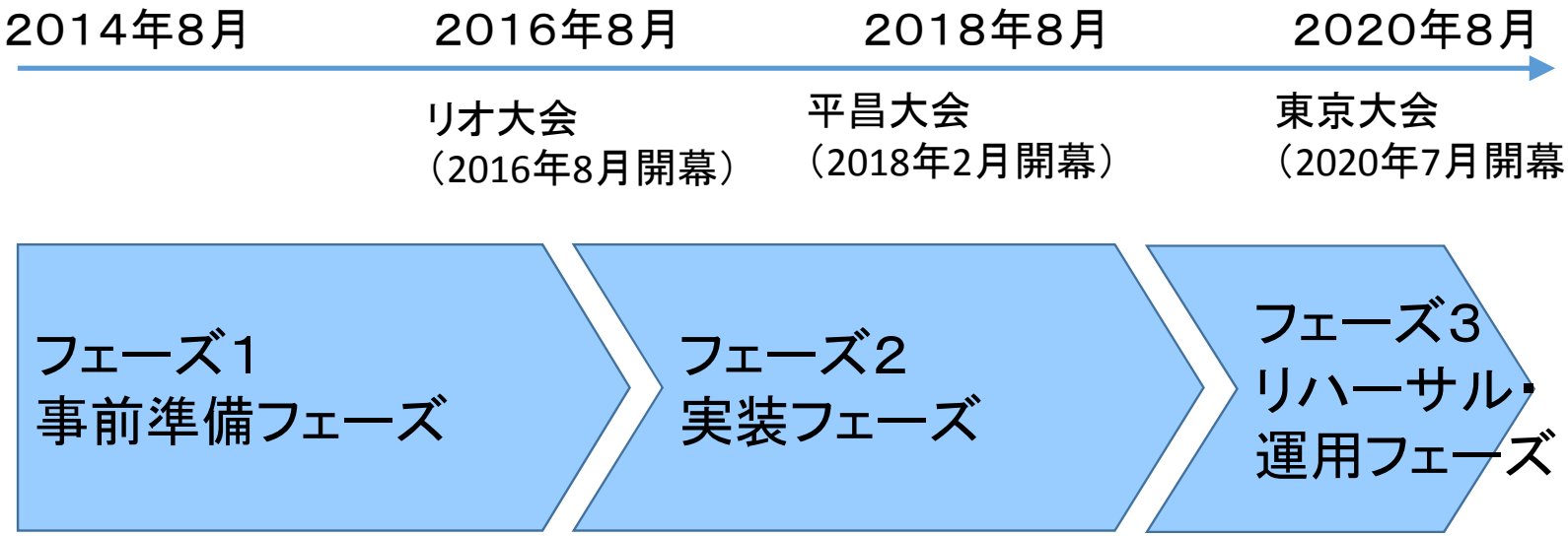
- ✓ まずはサイバーセキュリティに限定せず、**事業運営面・コミュニケーション面など多面的・体系的にリスク洗い出し・分析を行う体制**が必要。
  - ➢ 多人数でのブレーンストーミングは非効率であるため、作業は少人数グループに分割して実施することが望ましい。

システム・ネットワークに関するリスクの分類例



（注）本ページの記載内容は初期検討用の仮評価結果であり、実際の評価と異なる可能性があります。

2020年大会のサイバーセキュリティに関するロードマップ



- 関係機関とのコンセンサス形成（連携、役割分担など）
- リスク評価手法についての合意

- リスク評価の本格化
- システム・NW設計・運用設計への反映
- 関係機関での対策実装
- オリンピックCERT立上げ

- 実運用への移行
- テストイベント、リハーサルを通した実演習

4. サイバーセキュリティにおける大会のレガシーとは？（考察）

大会におけるレガシーとは？

- ✓『オリンピック競技大会のよい遺産（レガシー）を、開催都市ならびに開催国に残すことを推進する』

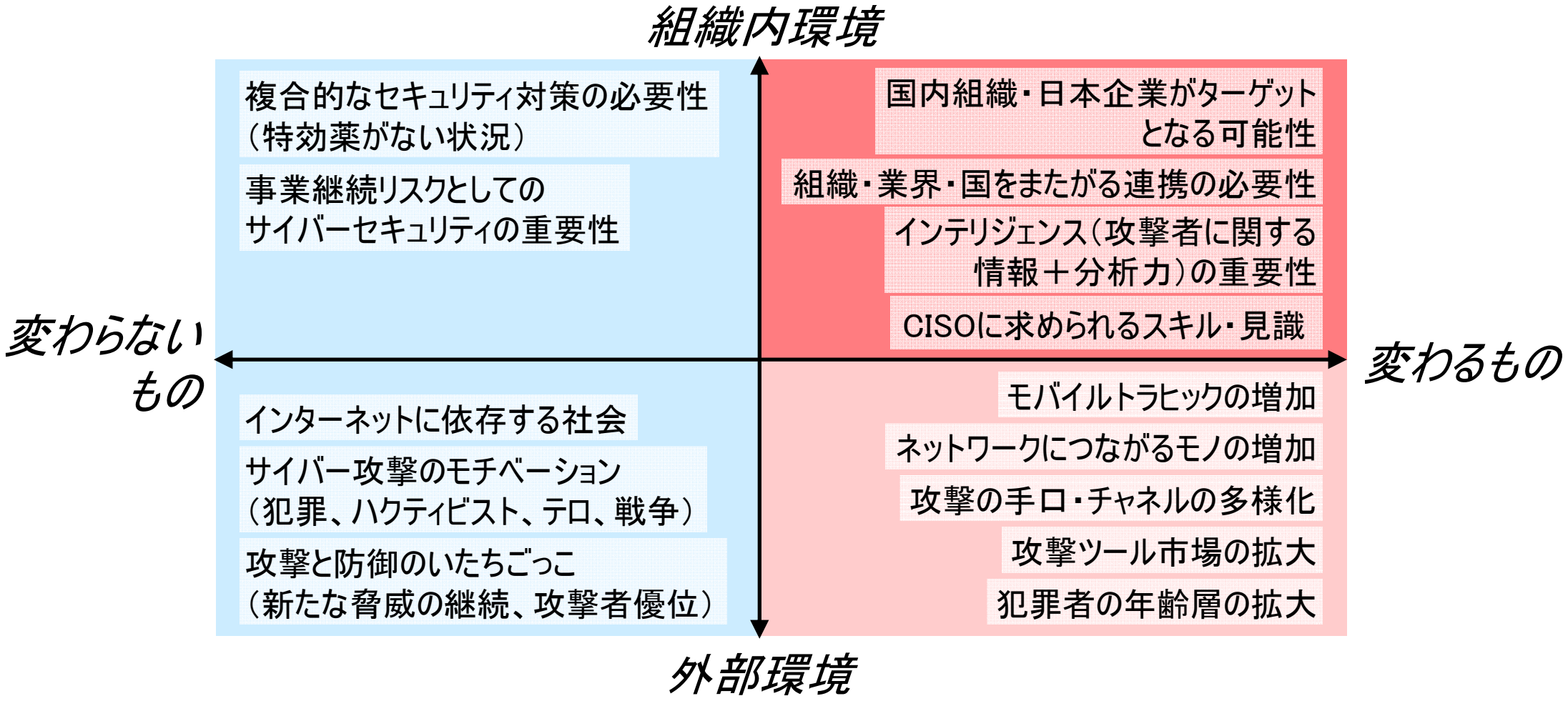
  （第1章「オリンピック・ムーブメントとその活動」第2項「IOCの使命と役割」）
- ✓『単に2020年に東京で行われるスポーツの大会としてだけでなく、2020年以降も含め、日本・世界全体に対し、様々な分野でポジティブなレガシーを残す大会とする。』

  （大会開催基本計画より）
- ✓ サイバーセキュリティにおける「2020年東京大会のレガシー」として何を目指すか？

サイバーセキュリティにおけるレガシーとは？

- ✓ ロンドン大会では、(1) 産業界や官公庁における格段のセキュリティ・レベルアップ、(2) 様々なレベルの教育プログラム、(3) 同分野をリードする大学の設定、(4) 官民連携、トレーニング、ペネトレテストなどの知見を海外輸出、(5) CERT-UKの設立 （英国政府の関係者による見解）
  - ➢ 金融業をはじめとする産業界のレベルアップ、国としてのサイバーテロ対策強化、などの側面で貢献している。
- ✓ 2020年大会をきっかけに、サイバーセキュリティ分野における日本・東京のブランドを確立すべく、官民あげて協力できないか。

2020年に向けて（おそらく）変わるもの、変わらないもの（例）

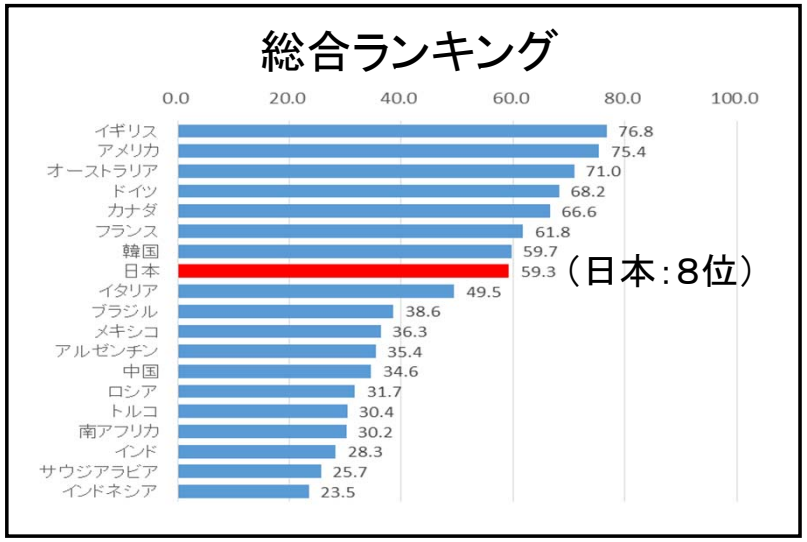


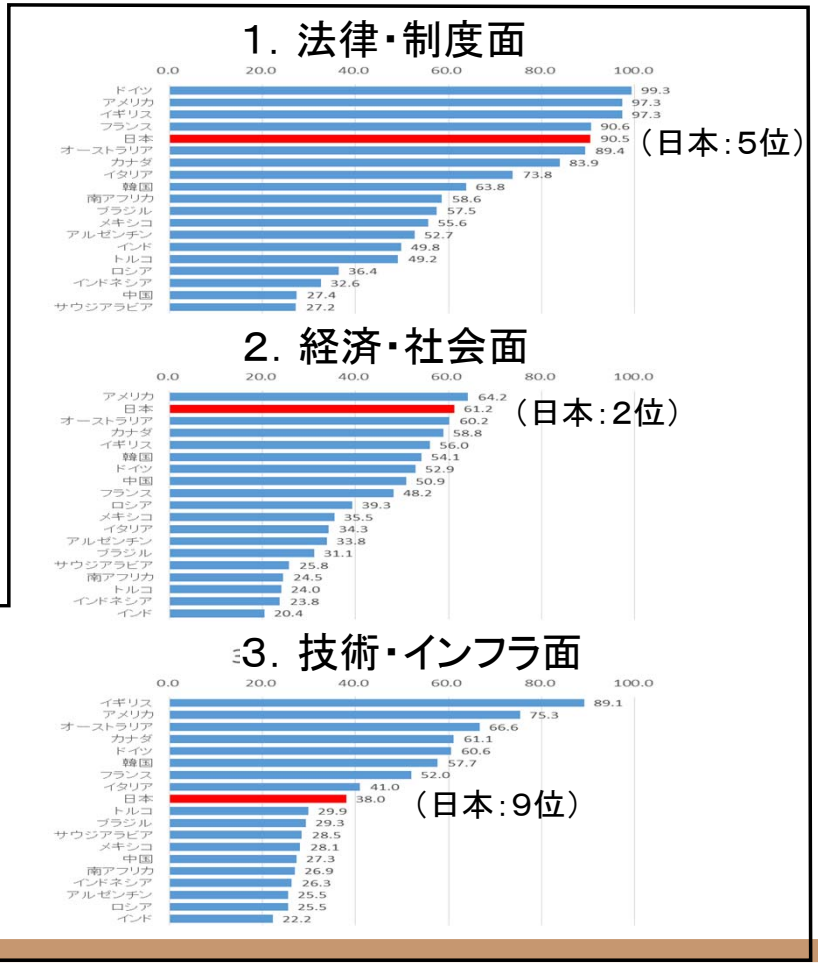
2020年に向けて（おそらく）変わるもの

- ✓ CISOの役割として、情報保護の観点からシステム・ネットワークに付随するリスクに着目するだけでなく、ビジネス全体に内在するリスク（たとえば情報セキュリティを強化することで情報活用が阻害されるリスク）を総合的に評価・判断することが求められる。（CISOからCIRO (Chief Information Risk Officer)へ）
- ✓ より効果的にビジネスを“守る”ために、より高度かつ包括的なインテリジェンスが求められる。（誰が何の目的で狙ってくるのか？組織に対してどのようなレピュテーションがあるのか？より有効な対策のために誰と組むべきか？）
- ✓ 将来のCSIRTは、もっと総合的な事業リスク管理部門になるのではないか。

【参考】Cyber Power Index

- 米国のコンサルティング会社、ブーズ・アレン・ハミルトン社が2011年に提唱した、サイバー分野の国力を評価する指標。





レガシーとしてのサイバー総合力（1/2）

- ✓ たとえばCyber Power Indexでは、４つのカテゴリー毎の評価と総合評価からなる。
  - ➢ 法律・規制面（政府のコミットメント、サイバー防御政策、検閲、政治的実行力、知的財産反故）
    ⇒日本：5位
  - ➢ 経済・社会面（教育水準、技術スキル、オープン性、ビジネス環境のイノベーションのレベル）
    ⇒日本：2位 （研究開発投資や特許出願数などを評価）
  - ➢ 技術インフラ面（ICT環境の利便性・品質・価格、ITへの投資、セキュアなサーバ数）
    ⇒日本：9位 （プリペイド携帯電話の普及率、通話料金（評価当時）などでマイナス評価）
  - ➢ 産業応用面（スマートグリッド、Eヘルス、Eコマース、ITS、Eガバメント）
    ⇒日本：9位 （ITS分野での評価は高いが、**全体的にまだ成長の余地が大きそう。。。**）

レガシーとしてのサイバー総合力 (2/2)

- ✓ たとえば産業応用面でより高いランクを目指すためには、情報やシステムを守ること（狭義のサイバーセキュリティ）に注力するだけでなく、**これからのIoT時代に備えてサイバー総合力（新しいIT技術を社会に取り込んでいく総合力）を強化**していく必要があるのではないでしょうか。
  - ➢ たとえばIT関連業界だけでなく、各業界ごとのISAC (Information Sharing and Analysis Center)活動や、業界横断的な情報交換がより活性化されるべきではないでしょうか。
  - ➢ たとえばベンダー目線（IT提供）だけでなく、ユーザ目線（IT活用）でITを社会やビジネスに取り込んでいくことを推進すべきではないでしょうか。

レガシーとしてのサイバー人材育成

- ✓ サイバーセキュリティ分野における“突出した人材”とは？
  - ➢ 「だれも考え付かなかった攻撃方法」「攻撃者のうらをかく斬新な防御手段」・・・ほとんど“クリエータ”の領域に近い、だからやっている本人は面白い。この人材がサイバーセキュリティの世界をリードしている。
- ✓ 一方でほとんどのビジネスを行う側から見れば、サイバーセキュリティはコストでしかない。いかにコストを減らして現業に集中できるか、にしか興味がない。
  - ➢ この認識で育成される人材とは、結局は“守ることができる人材”でしかない。
  - ➢ 「だれも考え付かなかったITの活用方法」「攻撃者の目線になりきった完璧な防御方法」を実現するには、クリエータを育成する必要がある。
- ✓ たとえば大会が終わった後の日本において、**サイバーセキュリティ人材（クリエータ）が社会や組織のIT化の中枢を支えるポストにつき、競争力の源泉として活躍するような絵姿**こそが、2020年のレガシーではないでしょうか。

最後に

- ✓ 2020年大会に向けた準備は、今後、内閣サイバーセキュリティセンターなど政府機関とも連携しつつ加速させていく予定です。
- ✓ 一方で、国を挙げての一大イベントだからこそ、大会の直接の関係者（組織委員会、スポンサー企業など）だけががんばってもうまくいかないというのは、サイバーセキュリティにも当てはまります。
- ✓ 業界全体・社会全体（さらには近隣諸国も交えて）で、大会・街・国を守っていく、サイバー総合力として一段のレベルアップを目指していく、という目的意識を醸成することが、一番の対策と考えます。
  - ➢ 『2020年大会の成功というのは共通の“目標”ではあるが、そこに関係する一人ひとりの“目的”はそれぞれ別にあるのではないでしょうか。』（組織委員会の某理事）

ご清聴ありがとうございました。